THE REVOLUTION IN MILITARY AFFAIRS AND CONFLICT SHORT OF WAR

Steven Metz
and
James Kievit

July 25, 1994

******

******

For ideas, comments, and background material, the authors would like to thank Rudolph C. Barnes Jr., Rod Paschall, William W. Mendel, Charles F. Swett, Jeffrey Cooper, Stefan Antonmattei III, Gary Guertner, Douglas V. Johnson, and, especially William T. Johnsen.

******

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA 17013-5050. Comments also may be conveyed directly to the authors by calling commercial (717) 245-3822 or DSN 242-3822, FAX (717) 245-3820, DSN 242-3820.

FOREWORD

For many experts on U.S. national security, the combination of emerging technology and innovative ideas seen in the Gulf War seem to herald a genuine revolution in military affairs. The victory of coalition forces demonstrated the technology and seemed to suggest that the revolution in military affairs can solve many of the strategic problems faced by the United States in the post-Cold War security environment.

In this study, the authors concede that the revolution in military affairs holds great promise for conventional, combined-arms warfare, but conclude that its potential value in conflict short of war, whether terrorism, insurgency, or violence associated with narcotrafficking, is not so clear-cut. Given this, national leaders and strategists should proceed cautiously and only after a full exploration of the ethical, political, and social implications of their decisions. To illustrate this, the authors develop a hypothetical future scenario--a "history" of U.S. efforts in conflict short of war during the first decade of the 21st century.

It is too early to offer concrete policy prescriptions for adapting many aspects of the revolution in military affairs to conflict short of war, but the authors do suggest an array of questions that should be debated. In order to decide whether to apply new technology and emerging concepts or *how* to employ them, the United States must first reach consensus on ultimate objectives and acceptable costs. The Strategic Studies Institute is pleased to offer this study as a first step in this process.

JOHN W. MOUNTCASTLE
Colonel, U.S. Army
Director, Strategic Studies Institute

BIOGRAPHICAL SKETCHES OF THE AUTHORS

STEVEN METZ is Associate Research Professor of National Security Affairs at the Strategic Studies Institute, U.S. Army War College. His specialties are transregional security issues and military operations other than war. Dr. Metz has taught at the Air War College, U.S. Army Command and General Staff College, and several universities. He holds a B.A. and M.A. in international studies from the University of South Carolina, and a Ph.D. in political science from the Johns Hopkins University. Dr. Metz has published many monographs and articles on world politics, military strategy, and national security policy.

JAMES KIEVIT is a Strategic Research Analyst at the Strategic Studies Institute, U.S. Army War College. His specialties are operational art, military engineering, and U.S. Army force structure issues. Commissioned in the Corps of Engineers, LTC Kievit has served in a variety of troop leading, command, and staff assignments in the 1st Cavalry Division, the 7th Engineer Brigade, and the 8th Infantry Division (Mechanized). He has also served as Assistant Professor of History at the U.S. Military Academy, and as a force structure analyst and study director at the U.S. Army Concepts Analysis Agency. LTC Kievit holds a B.S. from the U.S. Military Academy, a M.M.A.S. from the School of Advanced Military Studies of the U.S. Army Command and General Staff College, and a M.A. in history and M.S.E. in construction management from the University of Michigan.

SUMMARY

Many American strategic thinkers believe that we are in the beginning stages of a historical revolution in military affairs (RMA). This will not only change the nature of warfare, but also alter the global geopolitical balance.

To date, most attention has fallen on the opportunities provided by the RMA rather than its risks, costs, and unintended consequences. In the arena of conflict short of war, these risks, costs, and unintended consequences may outweigh the potential benefits.

The Strategic Context.

The Cold War notion of conflict short of war is obsolete. Politically and militarily, the Third World of the future will be full of danger. The future will most likely be dominated by peace enforcement in failed states, new forms of insurgency and terrorism, and "gray area phenomena." Many if not most Third World states will fragment into smaller units. Ungovernability and instability will be the norm with power dispersed among warlords, primal militias, and well-organized politico-criminal organizations. U.S. policy in the Third World is likely to be more selective and the U.S. homeland may no longer provide sanctuary. Renewed external support will restore the lagging proficiency of insurgents and terrorists.

The Application of Emerging Technology.

Emerging technology will have less impact on conflict short of war than on conventional, combined-arms warfare. It will, however, have some role. In noncombatant evacuation operations, new technology can assist with identification and notification of evacuees. Sensor technology, robotics, nonlethal weapons, and intelligence meshes will be used in combatting terrorism, countering narcotrafficking, and peace operations. These technologies, along with simulator training and unmanned aerial vehicles, will also be useful in insurgency and counterinsurgency.

Constraints and Countermeasures.

There are a number of constraints on applying the RMA to conflict short of war. These include the lack of a powerful institutional advocate for this process, a shortage of money for the development of technology specifically for conflict short of war, and the possibility that new technology may run counter to American values.

Enemies may also develop countermeasures to RMA innovations. Rather than attempt to match the technological prowess of U.S. forces, future enemies will probably seek asymmetrical countermeasures designed to strike at U.S. public support for engagement in conflict short of war, at the will of our friends and allies, or, in some cases, at deployed U.S. forces.

Making Revolution.

Rather than simply graft emerging technology to existing strategy, doctrine, organization, force structure, objectives, concepts, attitudes, and norms, the United States could pursue a full revolution in the way we approach conflict short of war. This is rife with hidden dangers and unintended consequences. A hypothetical future scenario illustrates some of these.

Conclusions and Recommendations.

In the near future, change will occur in the American approach to conflict short of war. To understand and control ongoing change, research, analysis, and debate is needed on a number of topics:

- A comprehensive general theory of military revolutions set within the context of broader notion of global politics and security;
- The strategy and policy foundation of military revolutions;
- The ethical dimension of RMA;
- The impact of the RMA on the structure of the U.S. national security organization;
- The impact of RMA on leader development within the military;
- The cultivation of appropriate expertise within the Army; and,
- Technology designed specifically for conflict short of war, especially psychological, biological, and defensive technology.

THE REVOLUTION IN MILITARY AFFAIRS AND CONFLICT SHORT OF WAR

Introduction: Groping for the Future.

In the late 1970s Soviet military analysts, led by Marshal N.V. Ogarkov, began to write of an emerging revolution in the nature of warfare.[1] By the early 1990s, this idea had spread to the United States, leading strategic thinkers inside and outside the government to conclude that ongoing innovation represents a true turning point in history.[2] If this is true, the strategic implications are far-reaching. Revolutionary changes in the character of warfare, according to Andrew F. Krepinevich, "have profound consequences for global and regional military balances."[3] But while it is clear that dramatic change is underway, its ultimate repercussions remain hidden.

In its purest sense, revolution brings change that is *permanent*, *fundamental*, and *rapid*. The basic premise of the revolution in military affairs (RMA) is simple: throughout history, warfare usually developed in an evolutionary fashion, but occasionally ideas and inventions combined to propel dramatic and decisive change. This not only affected the application of military force, but often altered the geopolitical balance in favor of those who mastered the new form of warfare. The stakes of military revolution are thus immense. Full of promise, it seems to offer Americans an answer to many enduring strategic dilemmas, whether intolerance of casualties, impatience, or the shrinking military manpower base. In a time of shrinking defense budgets, emerging technology may allow the United States to maintain or even enhance its global military power.[4] The Gulf War was widely seen as a foretaste of RMA warfare, offering quick victory with limited casualties. As a result, most attention has been on the *opportunities* provided by RMA rather than its *risks*, *costs*, and *unintended side effects*.

It is ironic that just as Marxism reached final bankruptcy as a framework for political and economic organization, one of its basic notions gained new life. Karl Marx, after all, postulated that revolutions can be *deliberate* rather than inadvertent; historical change can be created, engineered, and harnessed by those who understand it. Without direct attribution to Marx, this idea led many analysts to assume the current RMA can be the first deliberate one as senior military leaders and strategic thinkers consciously shape the future.

Whether Marxist or not, revolutionaries must always ask a series of key questions. First: Do the proper preconditions exist for revolutionary change or can they be created? In contemporary military affairs, the answer to this is "yes." Emerging technology; economic, political, and social trends; and, most importantly, new ideas create the right environment for revolution. Then revolutionaries must ask: How can I begin, sustain, and control the revolution? In current military affairs, this question is still under debate. Finally, the most difficult and often most critical questions are: Do we truly want a revolution? and, Will the long-term benefits outweigh the costs and risks? Advocates of a revolution in military affairs have not begun to grapple with these issues.

The change wrought by some revolutions is deep; others do not reach such extremes. This also applies to RMAs. The United States now faces a crucial choice. We can choose to drive the current RMA further and faster than any of its predecessors. In combined-arms warfare, this may be necessary. But conflict short of war--whether terrorism, narcotrafficking, peace enforcement, or insurgency--is different. Even if the RMA does prove applicable to these problems, there are good reasons for *deliberately* limiting it. As the United States faces this dilemma, strategic considerations rather than our fascination with technology and enthusiasm for change must be paramount.

Cry "Havoc!": The Strategic Context.

RMAs are born, develop, and die in specific strategic contexts, each composed of an array of social, economic, political, and military factors. The strategic context of the current RMA is dominated by the transformation of the global system from the Cold War to post-Cold War period. This shapes conflict short of war and influences the utility of U.S. military force.

During the Cold War, the most strategically significant form of conflict short of war-- then called "low-intensity conflict"--was revolutionary insurgency in the Third World. Low-intensity conflict outside the Third World did not require U.S. military force--the British, Italians, Germans, or Spanish could deal with their own problems--but revolutionary insurgency targeting our Third World allies often did. Using the strategy of protracted guerrilla war perfected by Mao and Giap, insurgents, usually supported by the Soviet Union, China, or their proxies, sought to overthrow fragile, pro-Western regimes. Because revolutionary insurgency thwarted political reform and economic development, often spread to neighboring states, and, when successful, increased Soviet influence, we considered it a major threat. Admittedly no Third World insurgency directly endangered the United States, but in combination they did. The dominant strategic logic was what French counterinsurgent theorists called "death by a thousand small cuts."[5]

In response, Western strategists developed an elaborate counterinsurgency doctrine. Codified by Robert Thompson, Roger Trinquier, and others, this initially emerged from the French and British experience in Malaya, Algeria, and Indochina.[6] Eventually Americans assumed responsibility for the counterinsurgency paradigm; Vietnam replaced Malaya and Algeria as the seminal event.[7] The culmination of Cold War-era thinking was the 1990 release of Field Manual (FM) 100-20/Air Force Pamphlet (AFP) 3-20, *Military Operations in Low Intensity Conflict*.[8] By defining counterinsurgency as opposition to Marxist "people's war," this document viewed low-intensity conflict in general as a subset of the struggle between the superpowers.[9] Regime legitimacy was the central concept. The United States sought to augment this and, ultimately, ameliorate the underlying causes of conflict. The military dimension of counterinsurgency simply allowed economic and political reforms to take root. Counterinsurgents could not win through purely military means, according to this theory, but they could lose.

Full of well-developed, impressive thinking, FM 100-20 deals with forms of violence rapidly becoming obsolete. Today, the essential nature of conflict short of war is changing. Marxist "people's war" represents the past. The future will most likely be dominated by peace enforcement in failed states, new forms of "spiritual" insurgency designed to radically alter the ideological structure of regimes, and "commercial" insurgency from quasi-political "gray area phenomena" such as narcoterrorism.[10] Other important changes are also on the way. During the Cold War, conflict short of war primarily concerned nation-states. In the post-Cold War era, many if not most Third World states will fragment into smaller units. Ungovernability and instability will be the norm. Even those which formally remain intact will see political and military power dispersed among warlords, primal militias, and well-organized politico-criminal organizations.[11] Most of these will be characterized by ruthlessness, some also by dangerous sophistication as terrorists and narcotraffickers master modern technology. Rapid, multilayered global communications will allow insurgents, terrorists, and narcotraffickers to learn and adapt quickly and even to form alliances and coalitions. While war or near-war may be no more common than in past decades, general, low-level violence will be pervasive.

In this environment, the United States will probably concentrate on containing rather than ameliorating conflict. Our future policy in the Third World is likely to be more selective with a trend toward disengagement. While the global conflict with the Soviet Union forced American engagement in Third World struggles where tangible national interests were minimal, the end of the Cold War gives us the option of limiting our role in certain types of conflicts to support of the United Nations or other multinational efforts, or rejecting involvement all together. While the great powers are currently cooperating on Third World conflict, they are likely to lose interest over the long-term. If this happens, U.S. objectives will increasingly be symbolic as we pursue humanitarian relief or attempt to cultivate a system of world order but are not willing to bear the costs of the final resolution of complex and long-standing conflicts.

Most ominously, the U.S. homeland may no longer provide sanctuary as it did from Cold War-era low intensity conflict. As in Great Britain, insurgents and terrorists angered by U.S. policy may bring the conflict to our country using global interdependence and the increased international flow of people. Moreover, as Third World dictators assimilate the lessons of the Gulf War, they will see conflict short of war as a useful but safer form of aggression. Renewed external support will restore the lagging proficiency of insurgents and terrorists including their technological capability. Politically and militarily, then, the Third World of the future will be full of danger.

Let Slip the Dogs of War: The Application of Emerging Technology.

The emerging RMA in mid- or high-intensity warfare is centered around the fusion of sophisticated remote sensing systems with extremely lethal, usually stand-off, precision-strike weapons systems and automation-assisted command, control, and communications (C^3). Trained with electronic simulations, virtual reality devices, and field exercises, this fusion is expected to allow smaller military forces to attain rapid, decisive results through synchronized, near-simultaneous operations throughout the breadth and depth of a theater of war.[12] The eventual result may be radically new forms of conventional warfare. With a few exceptions, however, the impact of the RMA on conflict short of war is far less clear.

Attacks or raids--which are doctrinal missions for the U.S. Army--are an exception. The military objective of attacks or raids in a conflict short of war is to damage or destroy high value targets of an adversary in order to seize and maintain the political or military initiative, and to demonstrate U.S. capability and resolve.[13] Although sometimes such operations are covert and executed by unconventional or special operations forces, in most cases a successful operation and its effects should be clearly visible to both the target and the international community. Emerging RMA technologies should improve the U.S. military's capability in these types of operations. Terrestrial, aerial, and space-based, autonomous, wide-ranging, high-speed collecting devices capable of on-board processing will identify precise targets and provide near-real-time information about the adversary's dispositions. Distributed interactive simulations and virtual reality devices will train the forces and be used to rehearse the strikes. And automation-assisted C^3 systems will synchronize and control lethal, stand-off, precision-guided weapons systems in near-simultaneous attacks.[14] Information technology could be used to both conceal the intent to strike and, later, provide evidence of a successful strike.[15] Attacks and raids during conflict short of war are, in effect, mid- to high-intensity operations writ small.[16] RMA therefore can have a significant effect. By contrast, the potential impact of emerging technology on more "traditional" operations in conflict short of war such as noncombatant evacuation operations (NEOs), counterterrorism, counternarcotrafficking, peace enforcement, and counterinsurgency is more ambiguous.

In the increasingly global economy, large numbers of Americans may find themselves in areas of instability and conflict. Voluntary and involuntary noncombatant evacuation operations will therefore be more frequent. The strategic objective of a NEO is the removal of U.S. (and occasionally allied) citizens from danger. The presence of Americans in areas of conflict reduces the flexibility of decision makers not only because U.S. citizens might be taken hostage or endangered, but also because their injury or death can rally public support in the United States for more militant action than policymakers might otherwise favor. But the open declaration of a NEO and its execution also restricts options since it signals the seriousness of a crisis by "clearing the decks" for further action. For decision makers this creates a tension between a desire to remove citizens from danger early and a fear of intensifying a crisis or precipitating undesirable adversary reaction.

While advances in robotics and information technologies may make it possible to perform many commercial activities with fewer employees in dangerous regions, those Americans who are overseas will be more isolated and dispersed. This complicates the main problems of NEOs: identification and notification of the individuals to be evacuated, identification of safe evacuation routes, and assessment of threats to the evacuation. Technology could diminish these problems. In the near future every American at risk could be equipped with an electronic individual position locator device (IPLD). The device, derived from the electronic bracelet used to control some criminal offenders or parolees, would continuously inform a central data bank of the individuals' locations. Eventually such a device could be permanently implanted under the skin, with automatic remote activation either upon departure from U.S. territory (while passing through the security screening system at the airport, for example) or by transmission of a NEO alert code to areas of conflict. Implantation would help preclude removal of the device (although, of course, some terrorists might be willing to remove a portion of the hostage's body if they knew where the device was implanted). The IPLD could also act as a form of IFFN (identification friend, foe, or neutral) if U.S. military personnel were equipped with appropriate challenge/response devices. Finally, such a device might eventually serve, like Dick Tracey's wrist radio, as a two-way communication channel permitting the NEO notification to be done covertly.

The second emerging technology with direct application in NEOs is the unmanned aerial vehicle (UAV). UAVs will be able to conduct rapid reconnaissance of possible evacuation routes and identify threats during the evacuation. Their small size will make them less conspicuous than either ground vehicles or manned air platforms. Large numbers of fast UAVs could cover multiple exit routes, thus complicating any attempt to interfere with the NEO. In combination with "wrist-radios," High Altitude Long Endurance (HALE) UAVs could provide NEO notification capability via scrambled TV/radio to Americans on the ground.[17] When a NEO required combat action, stand-off, precision-strike weapons systems could allow small military teams to accomplish missions which today require companies or even battalions.[18] Equipping these small units with adaptive camouflage could also reduce the visibility of NEOs.[19] The less visible an operation, the less provocative; the less visible military teams are, the harder to interfere with them.

Finally, developing military C^{3}I systems could help avoid dangerous, last minute evacuation of Americans all together. Currently, businessmen and diplomats facing crises tend to linger until the last possible moment, often ignoring official warnings. If the U.S. military could gain nondestructive access to (and perhaps even control of) the communications of an area from remote locations and made this available to Americans, businessmen and diplomats might voluntarily depart early in a crisis knowing they could carry on their activities even though not physically present. By encouraging voluntary departure prior to a crisis, reducing the need for a public disclosure of a NEO, and reducing the political visibility of evacuations, emerging technology increases options available to decision makers and reduces the degree to which NEOs act as barometers of U.S. resolve. When evacuees are actually threatened, the ability to strike quickly, precisely, and from a distance will provide a margin of safety.

Providing safety is also the primary U.S. objective when combatting terrorism. Currently, the State Department deals with terrorism overseas and the Federal Bureau of Investigation has domestic jurisdiction. The military supports both. Efforts to combat terrorism fall into two categories: *defensive* measures to reduce the vulnerability of individuals and property (antiterrorism), and *offensive* actions to prevent, deter, and punish (counterterrorism).[20] Emerging technologies are a two-edged sword. Some--like bio-technical weapons--can be tools of terrorism. Others--like precision, stand-off weapons or intrusive information technologies--may be used either for or against terrorism.

If technology allows a reduced American presence overseas, antiterrorism will be easier. Improved sensors and robotic guard systems may make installations, both military and commercial, more difficult to penetrate. In counterterrorism, according to Count de Marenches, former chief of French Intelligence, "Precision personal intelligence can be more critical than precision-guided munitions."[21] Advances in electronics and sensors and, even more importantly, the ability to fuse data through automation and improved organizations may provide that most critical commodity. New computer software, according to Alvin and Heidi Toffler, could "quickly discover and expose critical associations that would otherwise go undetected."[22] As demonstrated by Israel, UAVs can also play a significant role: "... a remotely piloted plane followed a car carrying fleeing terrorists back to their base, so that it could subsequently be demolished by air attack."[23] If the Army develops the aerial capability to broadcast and alter television signals, it could remove a key and essential weapon from the terrorist arsenal--media coverage.[24] Finally, some authors have speculated that advances in nonlethal weapons may make it possible to disable and capture terrorists or "glue" incoming car bombs to the street.

At least one analyst has suggested using "soft kill" weapons such as high energy radio frequency (HERF) guns and electromagnetic pulse transformer (EMP/T) bombs, to interdict narcotrafficking flights by damaging or destroying their avionics.[25] Like combatting terrorism, counternarcotrafficking operations are primarily a law enforcement function, with the military providing support.[26] Because narcotraffickers operate like terrorists, much counterterrorism technology can be used against them. In fact, narcotraffickers are even more likely than terrorists to rely on radios, cellular telephones, fax machines, and computers. This greatly increases their vulnerability to electronic intelligence gathering and disruption. For example, remote intrusive monitoring of the financial computer networks of offshore banks could identify the deposits associated with money laundering. If desired, such accounts could be electronically emptied.

Because interdicting narcotrafficking is similar to locating a military opponent's reconnaissance platforms, a military capable, in Martin Libicki's words, of collecting "more and more data about a battlefield, knitting a finer and finer mesh which can catch smaller and stealthier objects" could pinpoint intruders into U.S. territory.[27] Existing radar nets can identify aircraft attempting low altitude entry into the United States, so a favored technique of drug smugglers is to transfer the contraband from planes to speedboats offshore. Tracking and stopping high-speed small craft in coastal waters is difficult today. With projected advances in sensors and directed-energy or stand-off precision conventional munitions it could become routine. Drugs smuggled in commercial carriers might be interdicted by hosts of miniaturized, remote controlled, robotic detectors capable of rapid stem to stern searches of ships and airliners.[28] Interdiction of narcotics at the source, currently a resource-intensive activity involving search and destroy operations or large scale spraying of ecologically damaging herbicides, might be done in the future by miniature, self-mobile, bio-mechanical "bugs" delivered by aerial dispenser to seek out and kill or modify narcotic producing plants.[29] Alternatively, information warfare systems might influence the behavior of populations by convincing citizens to turn in traffickers or not buy drugs.

Behavior modification is a key component of peace enforcement. The primary objective of these operations is to prevent violence and facilitate diplomatic resolution of a conflict.[30] "Soft kill" systems can play a key role. Examples include not only information warfare but also biotechnical antimaterial agents which "could disable propulsion systems (attacking fuel and lubricants or clogging airways and critical passages); change the characteristics of soil or vegetation (to deny terrain to vehicles and troops); or degrade warfighting material (particularly those with organic components)."[31] Advances in electronics and robotics could also prove useful in peace operations, allowing commanders to separate forces with a "no man's land" populated by remote sensing devices or robotic patrols and enforced with stand-off precision strike weapons, thus reducing peacekeeper casualties and improving the chances that the peacekeeping force will remain long enough for a political resolution of the conflict.

The final area of consideration for application of emerging technologies to conflict short of war are insurgency and counterinsurgency. The military objectives of insurgency and counterinsurgency are diametrically opposed. In insurgency the United States assists an armed political organization attempting to seize power or extract political concessions from a regime opposed to U.S. interests. Counterinsurgency seeks to contain or defeat an insurgency attempting the overthrow of a friendly regime.[32] How then, might the RMA affect these operations? According to FM 100-20 the U.S. armed forces, when directed to do so, can assist insurgent efforts to:

- Recruit, organize, train, and equip forces;
- Develop institutions and infrastructure;
- Gather intelligence; and
- Perform psychological operations, surreptitious insertions, linkups, evasion, escape, subversion, sabotage, and resupply.[33]

Emerging technology can augment U.S. capabilities in a number of these areas. Simulator training devices can help force development and partially compensate for the difficulties insurgents face in performing actual field training. UAVs can be used for psychological operations aimed at mobilizing support and enhancing the legitimacy of the insurgents. Stealth vehicles can be used for insertions, biotechnological antimaterial agents for sabotage, and the U.S.'s extensive sensor and collector network can provide intelligence support.

Counterinsurgency is similar. Success hinges on obtaining accurate intelligence about the insurgents, and developing or maintaining government legitimacy. Greatly improved intelligence gathering and fusion is a primary component of the RMA, and proposed information warfare capabilities might be ideally suited for helping develop desired emotions, attitudes, or behavior.[34] Stand-off weapons could interdict outside support to the insurgents without requiring a U.S. presence. This could help a beleaguered regime maintain legitimacy. Improved training of security forces using simulators would improve their effectiveness, thus increasing the public's trust in the regime's ability to provide security.

Potholes in the Information Superhighway: Constraints and Countermeasures.

Emerging technology may improve the application of force in conflict short of war, but there is probably no imminent RMA in this arena. The changes in conflict short of war will be considerably less dramatic than in those projected for mid- to high-intensity combat, particularly when possible constraints or countermeasures are considered.

These constraints begin at the highest level as the basic nature of our national security organization generates obstacles to innovation. As Stephen Peter Rosen points out, large bureaucracies are not only difficult to change, they are explicitly designed *not* to change--"the absence of innovation is the rule, the natural state."[35] Ironically, the successful end of the Cold War, even though it dramatically increased the *need* for innovation, complicates the process. In all human endeavors, success tends to stifle innovation. The natural attitude is "if it ain't broke, don't fix it." The fact that the United States has not faced a recent military or national security disaster has hindered the development and application of new technology to conflict short of war. To many Americans, the absence of disaster shows that our national security strategy "ain't broke." Moreover, conflict short of war lacks a powerful institutional advocate able to transcend this attitude. Both civilian and military leaders in the Department of Defense fear that effort, time, and, most importantly, money spent on conflict short of war will be subtracted from that available for conventional combined-arms warfare. And it is not clear that the American public and the Congress consider improving our capabilities in conflict short of war important.

In this era of shrinking defense budgets, little money is available for technology designed specifically for conflict short of war. Fortunately, much of the technology developed for conventional mid- and high-intensity conflict can be extrapolated to conflict short of war, but insurgency, terrorism, and narcotrafficking also demand some unique capabilities. Like a business' investment in new plant, military technology increases effectiveness and efficiency in the long-term, but has major short-term costs. If we choose to engage in conflict short of war, two things could inspire efforts to develop and apply cutting-edge technology. One is the emergence of an active and powerful coterie of visionaries within the national security community, including both senior military and civilian leaders. The other is defeat or disaster. Yet even if the United States did make a concerted effort to apply emerging technology to conflict short of war, our opponents would quickly develop countermeasures, thus posing new problems and forcing further innovation by U.S. forces. Because U.S. engagement in conflict short of war will continue to be have weak domestic support, opponents will not have to match us innovation for innovation, but only increase the cost of American engagement beyond the low limits of public and congressional tolerance. How, then, might future opponents attempt to counter high-tech U.S. forces?

First, they will strike at domestic support for U.S. engagement. One way to do this is to kill Americans or damage U.S. property. Off-duty and rear-area U.S. forces in country will--as always--be targets. But in the increasingly mobile and interdependent world, the United States itself may also be vulnerable. At times, immigrant or resident alien communities within the United States may provide a base of support. New alliances among groups unhappy with our policy will coalesce, share information and, occasionally, conduct cooperative operations. Electronic terrorism--the sabotage of communications and computer systems in retaliation for official policy--will also be a tool of our enemies. Cyberspace will supplement international airports as the point-of-entry for terrorists. As a National Security Decision Directive signed by President Bush noted, "Telecommunications and information processing systems are highly susceptible to interception, unauthorized access, and related forms of technical exploitation...The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups..."[36] Opponents will also undercut domestic support for U.S. engagement through traditional political mobilization using immigrant and resident alien communities as well as sympathetic indigenous political groups--time-tested tactics honed during Vietnam and the 1980s. Advertising and public relations firms will be hired to construct sophisticated "consciousness-raising" campaigns. Often these will attack American public opinion indirectly by creating international opposition to our policy.

Opponents will also counter American military prowess by targeting our friends and allies. Reliance on allies has long been an American vulnerability in conflict short of war. In Vietnam, for example, even our hard-won understanding of revolutionary "people's war" could not bring victory to the incompetent and repressive Saigon elite. For American doctrine and strategy to work, we must have a local ally with some base of legitimacy.

Given this, future opponents may not even attempt to confront high-tech American forces, but instead steal a flank march by undercutting our allies. In conventional, combined-arms warfare, backward or weak contingents of coalitions can be assigned peripheral duties--figuratively holding the horses--and thus not erode the overall military effectiveness of the alliance. With the exception of operations in failed states or certain types of raids and attacks, a host nation must be the centerpiece of efforts to confront insurgency, terrorism, or narcotrafficking. The United States can be no more effective than its allies, a coalition no stronger than its weakest element. Terrorists, insurgents, and narcotraffickers will quickly recognize this.

In some cases, though, our opponents will attempt to directly counter deployed American forces. Since new technology will improve the ability of U.S. forces to locate and track enemies and to collect, analyze, and disseminate intelligence, the most useful countermeasures will be tactical, operational, and strategic camouflage and deception. Some opponents, especially those with an external sponsor, may deploy limited but high-tech methods of camouflage and deception. External sponsors may also provide just enough technology to their clients to foil our forces as Stingers did for the Afghan *mujahedeen*. Some narcotraffickers, insurgents, or terrorists will take a purely low-tech approach including things as simple as abandoning electronic communications in favor of written or voice messages, and relying on time-tested cellular organization to foil intelligence efforts.[37] Organizational decentralization may not totally destroy the effectiveness of RMA technology, but certainly erodes it. Saddam Hussein's Iraq or the other Third World caricatures of the Soviet Union are perfect opponents for a RMA-type military. Driven by the well-earned paranoia of tyrants, they have highly centralized military forces. This prevents coups d'etat, but also limits the chance of military victory against determined advanced states. Future insurgents, terrorists, and narcotraffickers will not be so stupid.

The use of new technology may also run counter to basic American values. Information age--and in particular information warfare--technologies cause concerns about privacy.[38] For example, the individual position locator raises several thorny issues: Would Americans overseas be forced to wear (or worse have implanted) such a device or would its use be voluntary? If forced, would it apply equally to those employed overseas and tourists? Will Americans accept the fact that the government might, by access to the NEO locator data base, know every move they make? If a locator device could be remotely activated, how could Americans be sure that activation was only effective outside the United States? How would they know that "wrist radios" were not used to monitor personal conversations? Similarly, military use of television against foreign adversaries raises the specter of domestic applications. Even if domestic use was never contemplated, its possibility might cause greater public skepticism regarding television appearances, reducing the impact of one of the American politician's greatest communication tools. Deception, while frequently of great military or political value, is thought of as somehow "un-American."

American values also make the use of directed energy weapons against suspected narcotrafficking aircraft technologically feasible but morally difficult, perhaps unacceptable. The advantage of directed energy weapons over conventional ones is deniability. Against whom is such deniability aimed? Certainly not the narcotraffickers, who will quickly recognize that interception by the Drug Enforcement Agency (DEA) or military planes leads to loss of their aircraft.[39] Instead, deniability must be aimed at the American people, who do not sanction the imprisonment, much less execution, of individuals without a trial (and execution is how they will perceive it--the argument "we only disabled the aircraft, it was the crash which killed the pilot" will carry little weight). Deniability will not last long, since narcotraffickers can choose any number of ways to make such interceptions public such as landing and then challenging the intercept technique in court, or arranging to relay communications with their aircraft to a ground station which could broadcast the "nonlethal" downing (ideally of a plane carrying no drugs). The American public may perceive the DEA or military involved in such actions to be as bad or worse than the narcotraffickers.

Certain biotechnical weapons--considered by some to violate the biological warfare convention to which the United States is a signatory--also may transgress American values regarding appropriate means.[40] Most Americans would not support the use of a weapon designed to target only a specific racial or ethnic group in anything less than a war for survival of the nation.[41] Could the government and military of this multi-ethnic republic face charges that it was developing or using a weapon targeting Africans, Jews, Koreans, Hispanics, etc.? Would defense against such a charge occupy the attention of policymakers to the detriment of other essential business? And even accidental injuries or deaths caused by "nonlethal" antimaterial substances could be politically damaging.

American values and attitudes thus form significant constraints on full use of emerging technology, at least in anything short of a perceived war for national survival. Overcoming these constraints to make a RMA in conflict short of war would require fundamental changes in the United States--an ethical and political revolution may be necessary to make a military revolution.

The Silicon Icarus: Making Revolution.

Even with all the constraints and countermeasures, there is some value in applying emerging technology using existing strategy, doctrine, organization, force structure, objectives, concepts, attitudes, and norms. But there is another alternative: we could deliberately engineer a comprehensive revolution, seeking utter transformation rather than simply an expeditious use of new technology. However alluring, such a program is rife with hidden dangers and unintended consequences. Unlike the architects of the Manhattan Project, we are not forced to pursue revolution without considering the implications. In conflict short of war, RMA is a Pandora's box desperately in need of careful scrutiny before opening.

But how to do so? Because it transcends the comfortable familiarity of both the past and present, revolution is never easy. It is, above all, a challenge to the imagination. Even the greatest revolutionaries have only hazy images of the future, their lives driven more by shadowy vision than concrete plans. But for decision makers contemplating revolution, visualizing long-term implications--however difficult--is the only way to gauge whether or not they truly want the kind of fundamental and irrevocable change revolution brings. To decide how far we want to push RMA in the arena of conflict short of war, Americans must speculate on where it might ultimately lead. One way to do this is by constructing hypothetical future scenarios. There are any number of feasible scenarios. The probability of any one is less important than the interconnections it uncovers. What follows, then, is such a hypothetical future scenario--a "history" of the application of RMA to conflict short of war written in the year 2010. It is not a prediction and certainly not a preference, but is a possibility.

> *The first question is: What led American leaders and national security professionals to apply the revolution in military affairs to conflict short of war? Most often, a revolution in military affairs occurs in response to defeat or a perception of rising threat. Napoleon led an undrilled army stripped of most veteran officers against a host of enemies; the architects of blitzkrieg all had first-hand experience with bitter military defeat. Likewise, the RMA of the 2000s was sparked by a series of fiascos in the mid-1990s. First was the emergence of what became known as "third wave terrorism." Recognizing the strategic bankruptcy of old-fashioned hijacking, kidnapping, assassination, and bombing, terrorists rapidly adopted state-of-the art technology to their sinister ends. Within Third World countries, they developed the means to identify and kill American businessmen, diplomats and military advisors at will, and to disrupt international air traffic and*

electronic communications in and out of their countries. Even more damaging was their ability to "carry the war to its source" in the United States. Biotechnology and information warfare, especially sabotage of communications and computer networks using mobile high power microwave sources, replaced AK-47s and SEMTEX as the preferred tools of terrorism. The new post-Mafia generation of silicon criminals provided models and even mentors for third wave terrorists.

About the same time, the U.S. military became embroiled in several horrific ethnic struggles. Our involvement usually began as part of a multinational peacekeeping or peace enforcement operation, but rapidly turned violent when American forces were killed or held hostage. The usual response to the first few attacks on Americans was to send reinforcements, thus placing U.S. prestige on the line. Since our strategy was contingent on global leadership, we were aware of the political damage which would result from being forcibly expelled from a Third World country, and thus doggedly "stayed the course" until domestic pressure forced withdrawal. On the ground, enemies would not directly fight our magnificent military forces, but relied instead on mines, assassination, and terror bombings.

The costs of these imbroglios were immense. A bitter dispute broke out in the United States between supporters of multinational peace operations and isolationists. And domestic political acrimony was not the only long-term cost of these operations: many of our troops assigned to operations in tropical areas brought back new resilient diseases which then gained a foothold in the United States. Debate was fierce over the new law requiring long-term quarantine of troops returning from Third World operations.

American efforts at counterinsurgency during the mid-1990s were no more successful. Whether facing commercial insurgents such as narcotraffickers or spiritual insurgents attempting to forge new systems of identity and personal meaning in their nations, we found that our allies were penetrated with enemy agents, corrupt, and unable to ameliorate the severe political, economic, and social problems that had given rise to insurgency. When a number of these allied governments collapsed, we were privately relieved but publicly aware of the precipitous decline in our prestige. At times, the United States tottered dangerously close to being the "poor, pitiful giant" Richard Nixon warned against.

In areas where the United States was not militarily involved, the major trends of the 1990s were the disintegration of nations, ungovernability, ecological decay, and persistent conflict. Much of this had a direct impact on the United States whether by generating waves of desperate immigrants, inspiring terrorists frustrated by our failure to solve their nations' problems, creating health and ecological problems which infiltrated the continental United States, or increasing divisiveness in the robustly multicultural American polity.

This series of fiascos led a small number of American political leaders, senior military officers, and national security experts to conclude that a revolution was needed in the way we approached conflict short of war. They held the Vietnam-inspired doctrine of the 1980s and 1990s directly responsible for these disasters. Only radical innovation, they concluded, could renew U.S. strategy and avoid a slide into the global irrelevance. Nearly everyone agreed the old strategic framework which coalesced in the 1960s was bankrupt. This thinking, derived from the Marshall Plan, sought to use American aid and advice to ameliorate the "root causes" of conflict in the Third World and build effective, legitimate governments. By the 1990s this was impossible or, at least, not worth the costs. Few, if any, Third World governments had the inherent capability of becoming stable and legitimate even with outside assistance.

The revolutionaries'first task was to recruit proselytes *throughout the government and national security community. Initially the revolutionaries, who called their new strategic concept "Dynamic Defense," were opposed by isolationists who felt that new technology should be used simply to build an impenetrable electronic and physical barrier around the United States. Eventually the revolutionaries convinced the president-elect following the campaign of 2000 that Dynamic Defense was both feasible and effective--a task made easier by his background as a pioneering entrepreneur in the computer-generated and controlled "perception-molding" systems developed by the advertising industry. The President was thus amenable to the use of the sort of psychotechnology which formed the core of the RMA in conflict short of war.*

The first step in implementing Dynamic Defense was reshaping the national security organization and its underlying attitudes and values. Technology provided opportunity; only intellectual change could consolidate it. With the full and active support of the President, the revolutionaries reorganized the American national security system to make maximum use of emerging technology and new ideas. This loosely reflected the earlier revolution in the world of business, and sought to make the U.S. national security organization more flexible and quicker to react to shifts in the global security environment. The old Cold War structures--the Department of Defense, Department of State, Central Intelligence Agency, National Security Council, and others--were replaced by two organizations. One controlled all U.S. actions designed to ***prevent*** *conflict, including economic assistance programs and peacetime diplomacy. The second was responsible for* ***containing*** *conflict by orchestrating sanctions, quarantines, embargoes, the building of multinational coalitions, and conflict short of war. This integrated the military, civilian law enforcement, the diplomatic corps, and organizations responsible for gathering and analyzing intelligence. Since so many of the conflicts faced by the United States were "gray area" threats falling somewhere in between traditional military problems and traditional law enforcement problems, the organizational division between the two was abolished. Moreover, many aspects of national security were civilianized or sub-contracted to save costs.*[42]

One of the most difficult dimensions of the reorganization was altering the dominant ethos of the armed forces. As technology changed the way force was applied, things such as personal courage, face-to-face leadership, and the "warfighter" mentality became irrelevant. Technological proficiency became the prime criterion for advancement within the military while the officer corps came to consider research universities such as Cal Tech and MIT its breeding ground rather than increasingly archaic institutions like West Point and Annapolis. For the military, the most common career track alternated assignments in national security with ones in business and science. Since physical endurance was not particularly important, military careers no longer ended after 20 or 30 years. In fact, soldiers and officers were given few responsibilities until the twentieth year of their careers. As proposed by Carl Builder, the Army was organized into highly specialized units permanently associated with a territorial franchise.[43] *Careers were within one of these units, thus allowing all soldiers and officers to develop the sort of language and cultural abilities previously limited to Special Forces and Foreign Area Officers.*

One of the turning points of the revolution came when its leaders convinced the President and key members of Congress that traditional American ethics were a major hinderance to the RMA. This was crucial: the revolutionaries and their allies then crafted the appropriate attitudinal vessel for the RMA. Through persistent efforts and very sophisticated domestic "consciousness-raising," old-fashioned notions of personal privacy and national sovereignty changed. This was relatively *easy since frustration with domestic crime had already begun to alter attitudes and values. In fact, the RMA in conflict short of war was, in many ways, a spin-off of the domestic "war on drugs and crime" of the late 1990s when the military, as predicted by William Mendel in 1994, became heavily involved in support to domestic law enforcement.*[44] *The changes in American values that accompanied that struggle were easily translated to the national security arena. Once the norms concerning personal privacy changed, law soon followed.*

Old-fashioned ideas about information control and scientific inquiry also changed. Preventing enemies (or potential enemies) from responding to our technological advantages became a prime objective of U.S. national security strategy. The government closely controlled and monitored foreign students attending American universities and exchanges of information within the global scientific and business communities. When necessary, the government protected valuable information through outright deception. And the national security community cooperated closely with business on counterespionage, providing training, advice, and equipment.

With values changed, technology then opened the door to profound innovation. Vast improvements in surveillance systems and information processing made it possible to monitor a large number of enemies (and potential enemies). In the pre-RMA days, psychological operations and psychological warfare were primitive. As they advanced into the electronic and bioelectronic era, it was necessary to rethink our ethical prohibitions on manipulating the minds of enemies (and potential enemies) both international and domestic. Cutting-edge pharmaceutical technology also provided tools for national security strategists.

Sometimes the revolutionaries found it necessary to stoke the development of technology designed specifically for conflict short of war. Whenever possible, profitability was used to encourage private and quasi-private enterprises to develop appropriate technology. For example, much of the lucrative technology of surveillance, intelligence collection, and attitude manipulation used to solve the domestic crime problem was easily adapted to conflict short of war. The same held for new weapons, especially nonlethal biological ones and advanced psychotechnology. Only when there was absolutely no expectation of profit did the government directly sponsor research of cutting-edge technology, often with funds freed by disbanding what were seen as increasingly irrelevant conventional military forces.

All of this reorganization and technological development was simply preface for the full flowering of the revolution in military affairs. American leaders popularized a new, more inclusive concept of national security. No distinction--legal or otherwise--was drawn between internal and external threats. In the interdependent 21st century world, such a differentiation was dangerously nostalgic. The new concept of security also included ecological, public health, electronic, psychological, and economic threats. Illegal immigrants carrying resistant strains of disease were considered every bit as dangerous as enemy soldiers. Actions which damaged the global ecology, even if they occurred outside the nominal borders of the United States, were seen as security threats which should be stopped by force if necessary. Computer hackers were enemies. Finally, external manipulation of the American public psychology was defined as a security threat.

The actual strategy built on the RMA was divided into three tracks. The first sought to perpetuate the revolution. Its internal dimension institutionalized the organizational and attitudinal changes that made the revolution possible, and pursued future breakthroughs in close conjunction with business, the scientific community, and local law enforcement agencies--the core troika of 21st century security. The external dimension actively sought to delay or prevent counterresponses *by controlling information and through well-orchestrated deception.*

The second track consisted of offensive action. Our preference was preemption. In a dangerous world, it was preferable to kill terrorists before they could damage the ecology or strike at the United States. While Americans had long supported this in theory, the RMA allowed us to actually do it with minimal risk just as the Industrial Revolution allowed 19th century strategists to build the massive militaries they had long desired. If regional conflicts--whether ethnic, racial, religious, or economic--did not damage the global ecology or appear likely to bring disease or violence to the United States, they were ignored. When conflicts seemed likely to generate direct challenges, the United States did not attempt ultimate resolution, but only to preempt and disrupt whatever aspect of the conflict seemed likely to endanger us. In the quest for strategic economy, preemption was the byword. Since the RMA made preemption quick, covert, usually successful, and politically acceptable, the United States gradually abandoned collective efforts. Nearly all allies, with their old-fashioned, pre-RMA militaries, proved more an encumbrance than a help. When preemption failed, the United States sought either passive containment which included isolation and quarantines, or active containment where strikes (electronic, psychological, or physical) were used to limit the spread of the deleterious effects of a conflict. For opponents with the ability to harm the United States, the military preemptively destroyed their capabilities.

The third track of the strategy was defensive, and included missile defense, cyberspace defense, and rigid immigration control.

By 2010, the RMA accomplished its desired objectives. Most of the time, we prevented Third World conflict from directly touching our shores. Probably the finest hour of the new warriors was the Cuba preemption of 2005--Operation Ceberus. This was so smooth, so effective that it warrants explanation. Following the overthrow of Fidel Castro in 1995 by a popular revolt, an elected government of national unity quickly proved unable to engineer massive economic and ecological reconstruction of the country or build a stable democracy. Frequent seizures of emergency powers and fraudulent elections were the rule. Within a few years, nostalgia for the stability of the old regime gave rise to an armed insurgency; most of the front-line rebels were former members of Castro's security forces and military. The United States refused to directly support the corrupt and inept regime, but recognized that the conflict required our attention.

The operation officially began when the President transferred the Cuban portfolio from the Conflict Preemption Agency to the Conflict Containment Agency. An existing contingency plan with implementing software provided the framework for quick action. Immediately, all electronic communication in and out of Cuba was surreptitiously transferred to the national security filter at Fort Meade. This allowed full monitoring, control, and, when necessary, manipulation of private, commercial, and government signals. Potential or possible supporters of the insurgency around the world were identified using the Comprehensive Interagency Integrated Database. These were categorized as "potential" or "active," with sophisticated computerized personality simulations used to develop, tailor, and focus psychological campaigns for each.

Individuals and organizations with active predilections to support the insurgency were targets of an elaborate global ruse using computer communications networks and appeals by a computer-generated insurgent leader. Real insurgent leaders who were identified were left in place so that sophisticated computer analysis of their contacts could be developed. Internecine conflict within the insurgent elite was engineered using psychotechnology. Psychological operations included traditional propaganda as well as more aggressive steps such as drug-

assisted subliminal conditioning. At the same time, Cubans within the United States and around the world were assigned maximum surveillance status to monitor their physical presence and communications webs. This thwarted several attempts to establish terrorist cells in the United States.

Within Cuba itself, fighting was widespread. Several acts of industrial and ecological terrorism led to the outbreak of disease. U.S. forces under the command of the Conflict Containment Agency helped control these while limiting the chance of their own infection by "stand-off" and robotic medical and humanitarian relief. Naturally all food supplies contained a super long-lasting sedative. This calmed local passions and led to an immediate decline in anti-regime activity. Where there were no direct U.S. relief efforts, sedatives were dispersed using cruise missiles. In areas thought to have high areas of insurgent activity, the dosage was increased.

Since all Americans in Cuba had been bioelectrically tagged and monitored during the initial stages of the conflict, the NEO went smoothly, including the mandatory health screening of all those returning to the United States. Coast Guard aircraft and hovercraft stanched illegal refugees. The attitude-shaping campaigns aimed at the American public, the global public, and the Cuban people went quite well, including those parts using computer-generated broadcasts by insurgent leaders--"morphing"-- in which they were shown as disoriented and psychotic. Subliminal messages surreptitiously integrated with Cuban television transmissions were also helpful.[45] *In fact, all of this was so successful that there were only a few instances of covert, stand-off military strikes when insurgent targets arose and government forces seemed on the verge of defeat. U.S. strike forces also attacked neutral targets to support the psychological campaign as computer-generated insurgent leaders claimed credit for the raids. At times, even the raids themselves were computer-invented "recreations." (These were a specialty of the Army's elite Sun Tzu Battalion.)*

Eventually it all worked: the insurgents were discredited and their war faded to simmering conflict unlikely to directly threaten the United States. Even the relatively unimportant criticism from domestic political groups was stilled when the President temporarily raised the quota of Cuban orphans eligible for adoption in the United States.

Unfortunately, there are growing signs in 2010 that the great advantages brought by the RMA might be eroding. With a decade to adapt, many opponents of the United States–both state and non-state actors–are themselves bending technology to their ends. While none can match the prowess of American forces across the board, indications are that by concentrating on one potential weakness of U.S. forces, enemies might be able to increase the human costs of intervention and, if not defeat the United States, at least deny us success. The RMA has amplified our distaste for death, a liability our enemies initially disdained and are now learning to manipulate in simple, low-tech ways.

In 2010, a decade of constant success in counterterrorism was marred by several dramatic failures. The post-attack environmental clean-up and reconstruction of St. Louis will take decades. Many of the difficult-to-detect drugs and psychotechnology developed for use in conflict short of war have appeared on the domestic black market and, increasingly, in American schools and workplaces. Perhaps most important, Americans are beginning to question the economic, human, and ethical costs of our new strategy. A political movement called the "New Humanitarianism" is growing, especially among Americans of non-European descent, and seems likely to play a major role in the presidential election of 2012. There are even rumblings of discontent within the national security community as the full meaning of the revolution becomes clear. Since the distinction between the military and non-military components of our national security community has eroded, *many of those notionally in the military service have to come to feel unbound by traditional notions of civil-military relations. This group has founded a new political party–The Eagle Movement–which is beginning to exert great pressure on the traditional political parties for inclusion in national policymaking. The traditional parties are, to put it lightly, intimidated by the Eagle Movement, and seem likely to accept its demands.*

In the end, only historians and philosophers of the future can ultimately assess the consequences of applying the RMA to conflict short of war.

Defining the Agenda: Conclusions and Recommendations.

The impact of purely military innovation, whether revolutionary or evolutionary, is nearly always less in conflict short of war than in warfare. The military dimension of conflict short of war is smaller, a less decisive proportion of the total struggle. Political, diplomatic, cultural, psychological, and economic factors matter in all conflicts, but are preeminent in conflict short of war. Military superiority–however measured–nearly always brings battlefield victory, but as Vietnam, Algeria, and a hundred other steamy struggles showed, it is not always strategically decisive in conflict short of war.

Still, there is some value in applying emerging technology and innovative concepts to conflict short of war. If the United States wants marginal improvements of effectiveness and efficiency, emerging technology and new concepts offer it. The bigger question is whether to seek true revolution rather than simply marginal improvements. To do so will demand fundamental changes in attitudes and values as well as organization, force structure, doctrine, and techniques. After serious debate, the people and leaders of the United States may decide the costs and risks of applying RMA to conflict short of war are not worth the expected benefits.

Even without such debate, undesirable change may come through accretion. By applying new technology here and new concepts there, by making apparently limited and benign modifications in the way we approach conflict short of war, by serendipity, we may eventually stumble into change as ultimately profound as deliberate revolution. Equally, revolutionary change in our approach to conflict short of war may come about *indirectly* as we grapple with domestic problems such as crime and drugs. If our traditional notions of privacy and public security are altered to fight these battles, it is an easy step to change our attitudes toward intervention in the affairs and psyches of foreign foes. Again, the focus on short-term considerations may lead to an undesirable future.

Whether we opt for revolution or evolution, change will occur. Our current approach to conflict short of war is a child of the Cold War. New threats demand new ideas; old assumptions no longer hold. To understand and control ongoing change, research, analysis, and debate is needed. Adaptation of military force structure, doctrine, and procedures must follow rather than precede this. The agenda for research, analysis, and debate, at least, is fairly clear.

For starters, we must develop a *comprehensive general theory of military revolutions* set within the context of broader notion of global politics and security. Currently, there is no accepted definition of RMAs or even agreement on which historical transformations constituted revolutions. It is not clear whether military revolutions are independent variables created by military leaders, or dependent variables that occur as spin-offs of wider social, political, and economic changes. We do not know conclusively whether military revolutions can be deliberately created, or whether rapid change is only seen as revolutionary after the fact. If the latter is true, then perhaps military revolutions are gist only for historians and not strategists. The concept of the "life-span" of a revolution–the period during which the enemy deliberately or inadvertently allows asymmetry to persist–also demands attention. What determines the "life-span"? Does military innovation increase the chances of conflict or diminish it? Finally, what is the relationship between the nature of future armed conflict and RMAs? Most of what are considered RMAs occurred in the Westphalian state system. Can they also occur in some different type of political system not based on nation-states and traditional inter-state war?

The *strategy and policy foundation of military revolutions* also warrants further study. Again, the direction of influence is central: Can military revolutions cause strategy to change, do strategic changes somehow generate military revolutions, or must they always occur simultaneously? Can an incomplete or partial military revolution occur in the absence of fundamental strategic change? Once these questions are answered, the architects of RMA must, if they are to gauge the potential for a military revolution, discern the future of U.S. strategy and policy in the Third World. American decision makers and strategists must then decide whether institutionalizing military revolution should be an integral part of our national security strategy in the absence of an equally innovative opponent like the Soviet Union.

Perhaps more importantly, analysis of *the ethical dimension of RMA* is needed. Military strategists often overlook the fact that the employment of force occurs within and is structured by an elaborate normative framework. This has a historical *foundation* based on just war theory, the Judeo- Christian ethical tradition, and international law as well as a *superstructure* constantly modified by specific military and political developments. In the 20th century total war, strategic bombing, nuclear weapons, limited war, and revolutionary people's war forced adaptation of the normative framework Americans use when employing force. The RMA will require a new assessment. We must decide whether innovative military capabilities are, in fact, acceptable and desirable. That can only happen through open debate. The military must be a vital participant, but not the sole one. But as the institution most intensely aware of both the opportunities and dangers offered by emerging technology and concepts, the military must–as our notion of civil-military relations evolves to meet changing conditions–serve as a catalyst of this debate.

We must also examine the impact of the revolution in military affairs on the *structure of the U.S. national security organization* including both the policymaking apparatus and the military services. Reflecting the Cold War strategic environment, the military services are each organized around a key warfighting competency defined by geographic medium–landpower dominance, air superiority, control of the seas, power projection on the oceanic littoral. If writers like Alvin Toffler and Winn Schwartau are correct and the key to future conflict is *information*, organization of the military by geographic medium may be obsolete.[46] At a minimum, the growing importance of information suggests the need for an integrated, interservice C^4I force.[47] The same logic holds for conflict short of war: since it must be confronted with a cohesive blend of military, political, economic, and intelligence assets, organizational integration makes sense. This notion bears careful analysis in the context of changes in the global security environment and emerging technology. Organizational change which was politically impossible or undesirable in the past should be considered anew.

The military services must also assess the impact of RMA on *leader development*. Since the Army plays the largest role of any service in conflict short of war, it must take the lead in this assessment. Based on a careful analysis of recent history, Stephen Rosen concludes that neither money nor outside encouragement determines the ability of a military to innovate. The key is acceptance by senior leaders that the nature of conflict is undergoing fundamental change. Then, Rosen argues, if "military leaders...attract talented young officers with great potential for promotion to a new way of war, and then...protect and promote them, they [can] produce new, usable military capabilities."[48] This suggests that the ultimate fate of the current revolution in military affairs will not be decided in the laboratories of the great universities, the board rooms of the major defense contractors, or even the offices of the Pentagon, but at Fort Leavenworth, in the classrooms of the Combined Arms Services and Staff School and the Command and General Staff College, and at PERSCOM.

The *cultivation of expertise* is related to leader development, but is not the same. Technological expertise should be of particular concern to the Army. Because of their roles and functions, the Air Force and Navy have traditionally emphasized technological expertise. For the Army, successful officers need branch-specific competence, interpersonal leadership and management ability, proficiency at staff functions, and, later in their careers, expertise at the operational and strategic levels of war. Technological acumen is relegated to a very few Army officers. But if an RMA is, in fact, underway, whether in conventional warfare or conflict short of war, and the Army intends to play a major role, it must develop a long-term program for cultivating technological expertise among all its officers rather than simply a tiny cadre. The same holds for nontechnological skills. If the Army is to pursue a RMA in conflict short of war, it must decide which nonmilitary skills from the worlds of law enforcement, science, intelligence, and psychology are necessary and then cultivate them throughout an officer's career. Research and analysis is also needed on *technology designed specifically for conflict short of war*. Currently, the primary advances of the RMA are in integrated, stand-off strike systems–the ability to find and destroy or disable targets by synchronized strike forces. Such capabilities form the heart of conventional, combined-arms warfare, but play only a very limited role in conflict short of war. Advances in sensors and other elements of information technology may bring great benefits to conventional, combined-arms warfare, but will have less impact in conflict short of war, which is most often won or lost through the manipulation of images, beliefs, attitudes, and perceptions.[49] These things rather than troop concentrations, command and control nodes, and transportation infrastructure are the key military targets in conflict short of war. This makes *psychological* technology much more important than strike technology. Ways must be found to use emerging technology, including advanced artificial intelligence and information dissemination systems, to help military strategists develop, implement, and continually improve methods of influencing opinion, mobilizing public support, and sometimes demobilizing it. There is also the potential for defensive pyschotechnology such as "strategic personality simulations" to aid national security decision makers.[50] To date, most analysts feel that the RMA has not generated adequate advances in such "soft war" capabilities or even the promise of such gains. But ultimate success in applying the RMA to conflict short of war hinges on the development of psychotechnology. As this emerges, it could be tested for political acceptability by using it first in non-lethal operations other than war like humanitarian relief and nation assistance.

Additional research is also needed on *defensive technology* for conflict short of war. Most current attention to defensive technology concerns protection against missiles. This is appropriate: ballistic missile proliferation poses a real and present danger to American national security. But in the arena of conflict short of war, different forms of strategic defense apply. For example, research is needed on the defense of cyberspace against politically-motivated terrorists.[51] As Winn Schwartau argues, the United States needs a national information policy to integrate the efforts of the national security community, business, and the criminal justice system.[52] And, as public health increasingly becomes a national security issue, strategic medical defense, including buffering the effects of ecological decay and preventing the import of new resilient diseases, demands study. Finally, research is needed on the application of *biotechnology* to conflict short of war. It is possible that some of the conceptual confusion concerning the current RMA may have to do with the compression of time which is such an integral characteristic of the modern era. In the past, RMAs took years, often decades to develop. Today, two RMAs may be underway simultaneously. The first (and more mature) is electronic. Its manifestations are improved C^4I and precision strike systems. The second (and potentially more profound) RMA is biotechnological, including genetic engineering and advanced behavior-altering drugs. Because of the compression of time and the shortening of historical patterns, the biotechnical revolution is totally enmeshed with the electronic. It may ultimately be the combination of the two that proves truly revolutionary.

****

Distilled to their essence, revolutions are acts of supreme creativity. The U.S. military is not inherently hostile to creativity, but is cautious. If the nation–our political and intellectual leaders and the public–decide that improving American capabilities in conflict short of war is necessary and desirable, the preeminent task for the military is to continue to build and enlarge a culture of creativity and strategic entrepreneurship among the officer corps. To some extent, this has begun. The changes leading to AirLand Battle, victory in the Gulf War, and the current RMA were supremely creative. Still, these were only first steps. To make a revolution in conflict short of war will be more difficult. But to allow technology to develop without concomitant creativity would, in the end, endanger the Nation's security.

ENDNOTES.

1. Jeffrey R. Cooper, "Another View of the Revolution in Military Affairs," a paper presented at the Fifth Annual Conference on Strategy, U.S. Army War College, Carlisle Barracks, PA, April 27, 1994, pp. 42-43.

2. See, for example, reports of the roundtables on the revolution in military affairs held for the Army, Air Force, and Navy by Science Applications International Corporation of McLean, VA, and Michael J. Mazarr, et. al., *The Military Technical Revolution*, Final Report of a CSIS Study, Washington, DC: CSIS, March 1993. Another important early work was Andrew F. Krepinevich, Jr., "The Military-Technical Revolution: A Preliminary Assessment," a report prepared for the Office of the Secretary Defense/Net Assessment (OSD/NA), July 1992.

3. Andrew F. Krepinevich, Jr., "The Coming Revolution in the Nature of Conflict: An American Perspective," in *The US Air Force Roundtable on the Revolution in Military Affairs*, a report prepared by Science Applications International Corporation, January 1994, p. 2.

4. Dan Gouré, "Is There a Military-Technical Revolution in America's Future?" *Washington Quarterly*, Vol. 16, No. 4, Autumn 1993, p. 175.

5. John Shy and Thomas W. Collier, "Revolutionary War," in Peter Paret, ed., *Makers of Modern Strategy From Machiavelli to the Nuclear Age*, Princeton, NJ: Princeton University Press, 1986, p. 852.

6. See Robert Thompson, *Defeating Communist Insurgency*, New York: Praeger, 1966; and Roger Trinquier, *Modern Warfare: A French View of Counterinsurgency*, New York: Praeger, 1967.

7. On the development of American counterinsurgency doctrine, see especially Douglas S. Blaufarb, *The Counterinsurgency Era*, New York: Free Press, 1977; Larry E. Cable, *Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War,* New York: New York University Press, 1986; and, D. Michael Shafer, *Deadly Paradigms: The Failure of U.S. Counterinsurgency Policy*, Princeton, NJ: Princeton University Press, 1988.

8. FM (Field Manual) 100-20/AFP (Air Force Pamphlet) 3-20, *Military Operations in Low Intensity Conflict,* Washington, DC: Headquarters, Departments of the Army and the Air Force, December 5, 1990.

9. *Ibid.*, pp. 2-7 through 2-14.

10. On the concepts of commercial and spiritual insurgency, see Steven Metz, *The Future of Insurgency*, Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1994.

11. For detailed analysis, see Steven Metz, *America and the Third World: Strategic Alternatives and Military Implications*, Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1994, pp. 12-24.

12. See, for example, Gordon R. Sullivan and James M. Dubik, *Land Warfare in the 21st Century*, Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1993. Also the reports of the roundtables on the revolution in military affairs held for the Army, Air Force, and Navy by Science Applications International Corporation of McClean, VA.

13. FM (Field Manual) 100-5, *Operations*, Washington, DC: Headquarters, Department of the Army, 1993, p. 13-8.

14. These are the capabilities identified as essential to future reconnaissance, surveillance, and target acquisition (RSTA) technologies in the Army's final draft Training and Doctrine Command (TRADOC) Pamphlet 525-xx, *Concept for Information Operations*, Ft. Monroe, VA: U.S. Army Training and Doctrine Command, May 5, 1994, p. 4-7.

15. Although the Army's most recent proposed doctrine in regard to Information Operations merely states: "The Army supports the timely and accurate release of information to the media as well as open and independent reporting as the principal means of coverage of U.S. military operations." TRADOC Pamphlet 525-xx, p. 2-9.

16. FM 100-20, pp. 5-5 to 5-7.

17. National Research Council, *STAR 21 (Strategic Technologies for the Army of the Twenty-first Century), Airborne Systems*, Washington DC: National Academy Press, 1993, pp. 49-55. Also Chuck de Caro, "Sats, Lies, and Video-Rape: The Soft War Handbook," unpublished paper, Aerobureau Corporation, 1994.

18. See for example the discussion in National Research Council, *STAR 21, Airborne Systems*, p. 19.

19. "Chameleon" camouflage is based on commercially available heat- and light-sensitive colorants that adapt to the surrounding environment, as well as electrically stimulated colorants that change color according to the surrounding landscape. See "Living Camouflage," *Soldiers' Magazine*, Volume 49, No. 3, March 1994, p. 9. Also National Research Council, *STAR 21, Special Technologies and Systems*, Washington DC: National Academy Press, 1993, pp. 23-24.

20. FM 100-5, pp. 13-6 and 13-7.

21. Quoted in Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*, Boston: Little, Brown, 1993, p. 157.

22. *Ibid.*, p. 157.

23. *Ibid.*, p. 113.

24. de Caro, "Sats, Lies, and Video-Rape," pp. 32-34.

25. Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, New York: Thunder's Mouth, 1994, pp. 171-176. Note that de Caro defines "soft war" as the hostile utilization of global television. "Soft kill" is used here in a more generic sense of any system designed to achieve its effect without causing harm to human beings. See National Research Council, *STAR 21, Technology Forecast Assessments*, p. 314.

26. FM 100-5, p. 13-6 .

27. Martin C. Libicki, *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, Washington, DC: National Defense University Institute for National Strategic Studies, March 1994, p. 24. The utility of Libicki's very interesting analysis is limited by his failure to provide supporting references.

28. For a brief description of very small autonomous systems, see Richard O. Hundley and Eugene C. Gritton, *Future Technology-Driven Revolutions in Military Operations: Results of a Workshop*, Santa Monica, CA: RAND Corporation, November 1993, pp. 12-37.

29. Possible advances in biotechnology are outlined in *STAR 21, Technology Forecast Assessments*, Washington DC: National Academy Press, 1993, pp. 314-346.

30. FM 100-5, p. 13-7.

31. National Research Council, *STAR 21, Technology Forecast Assessments*, Washington DC: National Academy Press, 1993, p. 346.

32. FM 100-20, p. 2-0 and pp. 2-7 to 2-9.

33. *Ibid.*, pp. 2-17 to 2-18.

34. *Ibid.*, p. 2-22.

35. Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military*, Ithica, NY: Cornell University Press, 1991, p. 5.

36. Quoted in Schwartau, *Information Warfare*, p. 127.

37. A classic explanation of cellular organization by insurgents is Andrew R. Molnar, *Human Factors Considerations of Undergrounds in Insurgencies*, Washington, DC: American University Center for Research in Social Systems, 1966, pp. 3-22.

38. See, as an example, Stephen Sloan, "Technology and Terrorism: Privatizing Public Violence," *Technology and Society*, Vol. 10, No. 2, Summer 1991, pp. 8-14.

39. Narcotraffickers may, in fact, respond by arming their own aircraft with conventional air-to-air weaponry. Imagine the surprise of the first DEA crew who sees, as they pass ahead of a suspected drug laden aircraft to aim their HERF gun at its vulnerable avionics, a Sidewinder exiting a

concealed cargo compartment.

40. The Army contends that its research falls within the limitations of the chemical and biological conventions. See National Research Council, *STAR 21, Technology Forecast Assessments*, pp. 314-315.

41. Tofflers, *War and Anti-War*, p. 122.

42. Michael Mazarr, an early analyst of the revolution in military affairs, considered "civilianization of war" one of the principles of the RMA. See *The Revolution in Military Affairs: A Framework for Defense Planning*, Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute, 1994, pp. 22-27.

43. Carl Builder, "Information Technologies and the Future of Conflict," Briefing to the Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (OASDSOLIC), March 23, 1994.

44. William W. Mendel, "The Cold War Returns," *Military Review*, Vol. 74, No. 5, May 1994, pp. 69-71.

45. This is described in Rod Paschall, *LIC 2010: Special Operations and Unconventional Warfare in the Next Century*, Washington: Brassey's, 1990, pp. 56-57.

46. Tofflers, *War and Anti-War*; Schwartau, *Information Warfare*.

47. For a detailed discussion, see Libicki, *The Mesh and the Net*, pp. 52-69.

48. Rosen, *Winning the Next War*, p. 252.

49. By contrast, a seminal study by the Center for Strategic and International Studies suggests that emerging sensor technologies (at least) will have equal benefits for conventional and unconventional military operations. (Mazarr, *et. al.*, *The Military Technical Revolution*, p. 44.)

50. See Norman D. Livergood and Stephen D. Williams, "Strategic Personality Simulation: A New Strategic Concept," unpublished draft paper, Carlisle Barracks, PA: U.S. Army War College, 1994.

51. For thinking on this topic, see Hundley and Gritton, *Future Technology-Driven Revolutions in Military Operations*, pp. 60-73.

52. Schwartau, *Information Warfare*, pp. 316-353.

U.S. ARMY WAR COLLEGE
Major General William A. Stofft
Commandant
****
STRATEGIC STUDIES INSTITUTE

Director
Colonel John W. Mountcastle

Director of Research
Dr. Earl H. Tilford, Jr.

Authors
Dr. Steven Metz
Lieutenant Colonel James Kievit

Editor
Mrs. Marianne P. Cowling

Secretary
Mrs. Shirley E. Martin
****
Cover Design
Mr. James E. Kistler

Composition
Mr. Daniel B. Barnett